PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-318734

(43)Date of publication of application : 31.10.2002

(51)Int.Cl. G06F 13/00
G06F 11/34
G06F 15/00

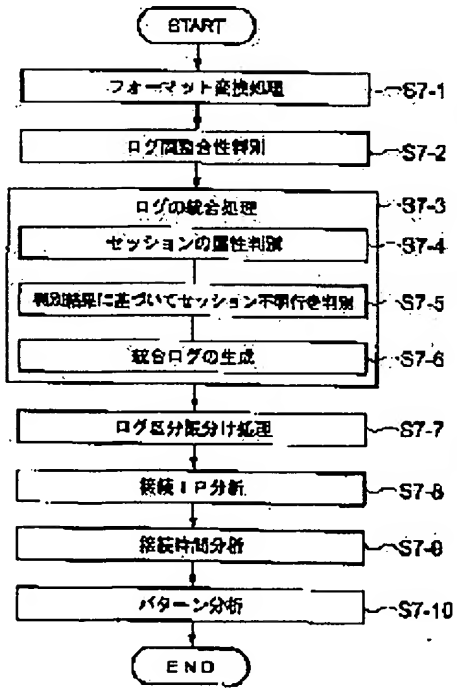
(21)Application number : 2001-120308

(22)Date of filing : 18.04.2001

(71)Applicant : TEAMGIA:KK

(72)Inventor : ABE HIROKI

(54) METHOD AND SYSTEM FOR PROCESSING COMMUNICATION LOG



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and a system for processing communication log, with which unauthorized access or the like can be discovered without requesting application or experience to a security manager.

SOLUTION: This method has a process (a) for converting each of analysis object log files outputted by an application capable of recording a plurality of communication logs to a prescribed format as needed, a process (b) for merging a plurality of analysis object logs converted into the prescribed format and a process (c) for judging the presence/absence of the unauthorized access by analyzing the merged log.

* NOTICES *

CLAIMS

[Claim(s)]

[Claim 1]A communication log disposal method comprising:

(a) A process of carrying out the conversion process of each analysis object log file which application which can record two or more communication logs outputted to a predetermined format when required.

(b) A process of unifying two or more analysis object logs changed into said predetermined format.

(c) A process of judging existence of unlawful access by analyzing a log after being unified.

[Claim 2]A log communication processing method, wherein said two or more analysis object log files are recorded about the same system in the communication log disposal method according to claim 1.

[Claim 3]A communication log disposal method having further the process of distinguishing compatibility between said two or more analysis object logs, and outputting the discriminated result before the (d) aforementioned (a) process or the (b) process in the communication log disposal method according to claim 2.

[Claim 4]In the communication log disposal method according to claim 1, the aforementioned (a) process, A communication log disposal method being what has the process of changing said analysis object log file into a predetermined format, using a conversion procedure which outputted said analysis object log file, and which was beforehand prepared for every application.

[Claim 5]A communication log disposal method having further the process of updating a conversion procedure beforehand prepared for said every application to predetermined timing in the communication log disposal method according to claim 1.

[Claim 6]A communication log disposal method having further the process of classifying a line which belongs from said analysis object log before the (e) aforementioned (a) process or the (b) process at the same session in the communication log disposal method according to claim 1.

[Claim 7]A communication log disposal method to which a line which cannot distinguish the session which belongs is characterized by having further the process of distinguishing to which session it belonging based on a line from which the aforementioned (e) process can distinguish the session which belongs among an analysis object log in the communication log disposal method according to claim 6.

[Claim 8]A communication log disposal method characterized by the aforementioned (b) process being what unifies said two or more analysis object logs for every same session in the communication log disposal method according to claim 1.

[Claim 9]A communication log disposal method characterized by the aforementioned (c) process being what distinguishes existence of unlawful access for every analysis object log integrated for said every same session in the communication log disposal method according to claim 8.

[Claim 10]A communication log disposal method characterized by the aforementioned (c) process being

which can record two or more communication logs outputted to a predetermined format when required.
(b) A means to unify two or more analysis object logs changed into said predetermined format.
(c) A means to judge existence of unlawful access by analyzing a log after being unified.

[Claim 12]A log communication processing system, wherein said two or more analysis object log files are recorded about the same system in the communication log processing system according to claim 11.
[Claim 13]A communication log processing system having further a means to distinguish compatibility between analysis object logs of the (d) aforementioned plurality, and to output the discriminated result in the communication log processing system according to claim 12.
[Claim 14]In the communication log processing system according to claim 11, the aforementioned (a) means, A communication log processing system being what has a means to change said analysis object log file into a predetermined format, using a conversion procedure which outputted said analysis object log file, and which was beforehand prepared for every application.
[Claim 15]A communication log processing system having further a means to update a conversion procedure beforehand prepared for said every application to predetermined timing in the communication log processing system according to claim 11.
[Claim 16]A communication log processing system having further a means to classify a line belonging to the same session from the (e) aforementioned analysis object log in the communication log processing system according to claim 11.
[Claim 17]In the communication log processing system according to claim 16, the aforementioned (e) means, A communication log processing system having further a means to distinguish to which session a line which cannot distinguish the session which belongs belongs based on a line which can distinguish the session which belongs among an analysis object log.
[Claim 18]A communication log processing system characterized by the aforementioned (b) means being what unifies said two or more analysis object logs for every same session in the communication log processing system according to claim 11.
[Claim 19]A communication log processing system characterized by the aforementioned (c) means being what distinguishes existence of unlawful access for every analysis object log integrated for said every same session in the communication log processing system according to claim 18.
[Claim 20]A communication log processing system characterized by the aforementioned (c) means being what classifies by color and displays the possibility of unlawful access for said every session in the communication log processing system according to claim 19.
[Claim 21]Computer software program products which collaborate with operation system installed in a computer system, and perform analysis processing of a communication log, comprising:
A storage.
(a) A means which carries out the conversion process of each analysis object log file which it was stored in

(c) A means to judge existence of unlawful access by being stored in said storage and analyzing a log after being unified.

[Claim 22]A log communication processing system, wherein said two or more analysis object log files are recorded about the same system in the computer software program product according to claim 21.

[Claim 23]Computer software program products having further a means to be stored in the (d) aforementioned storage, to distinguish compatibility between said two or more analysis object logs in the computer software program products according to claim 22, and to output the discriminated result.

[Claim 24]In the computer software program product according to claim 21, the aforementioned (a) means, Computer software program products being what has a means to change said analysis object log file into a predetermined format, using a conversion procedure which outputted said analysis object log file, and which was beforehand prepared for every application.

[Claim 25]Computer software program products having further a means to update a conversion procedure beforehand prepared for said every application to predetermined timing in the computer software program products according to claim 21.

[Claim 26]Computer software program products which are stored in the (e) aforementioned storage in the computer software program products according to claim 21, and are characterized by having further a means to classify a line belonging to the same session from said analysis object log.

[Claim 27]In the computer software program product according to claim 26, the aforementioned (e) means, Computer software program products having further a means to distinguish to which session a line which cannot distinguish the session which belongs belongs based on a line which can distinguish the session which belongs among an analysis object log.

[Claim 28]Computer software program products characterized by the aforementioned (b) means being what unifies said two or more analysis object logs for every same session in the computer software program products according to claim 21.

[Claim 29]Computer software program products characterized by the aforementioned (c) means being what distinguishes existence of unlawful access for every analysis object log integrated for said every same session in the computer software program products according to claim 28.

[Claim 30]Computer software program products characterized by the aforementioned (c) means being what classifies by color and displays the possibility of unlawful access for said every session in the computer software program products according to claim 29.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

two or more log outputs are possible can be analyzed systematically etc.

[0002]

[Description of the Prior Art]The incidents in which the network and server of a company or government and municipal offices are attacked by a cracker etc. these days are occurring frequently. Attentions have gathered for strengthening of network security by this. In order to strengthen network security, it is necessary to supervise and analyze network security first. It is effective in the surveillance of network security to record and analyze the communication log of devices, such as a server which constitutes a network.

[0003]Communication histories, such as a server, are recorded, and this communication log is analyzing this and can detect all the phenomena which happened to this server. For example, it is detectable that there was unlawful access based on there having been unnatural access from the exterior to said server. Therefore, network security can be strengthened with forming a certain measure according to this.

[0004]

[Problem(s) to be Solved by the Invention]However, the log usually outputted from a server is recorded in a format different, respectively by OS and the application currently used of the computer, and is various. Since the quantity is too much huge, it is common that the network is employed in the state where time whether the contents can be checked and for checking is not securable and where there is a system management top problem.

[0005]Since the cracker which devises an attack to a network alters or deletes said log in order to eliminate the trace of network penetration of self, it is very difficult to discover such unlawful access in this case.

[0006]This invention is made in view of such a situation, and is a thing.

The purpose is to provide the log processing method and system which can discover unlawful access etc. without requiring advanced knowledge and experience of a person.

[0007]

[Means for Solving the Problem]A process of carrying out the conversion process of each analysis object log file which application which can record a communication log of (a) plurality outputted to a predetermined format according to the 1st main viewpoint of this invention when required in order to solve an aforementioned problem, (b) A communication log disposal method having a process of unifying two or more analysis object logs changed into said predetermined format, and the process of judging existence of unlawful access by analyzing a log after (c) integration was carried out is provided.

[0008]According to such composition, a format of two or more log files is unified by a method which was able to be defined for every log file, and it becomes possible to detect unlawful access which cannot be distinguished with an independent log file by unifying them.

[0009]Here, as for said two or more analysis object log files, according to the embodiment of 1 of this

files according to such composition, it can be distinguished by unifying these whether it is that in which an event in the system concerned includes unlawful access. It is detectable by distinguishing compatibility during two or more files that a part of files were altered.

[0011]If it depends like 1 operative condition, the aforementioned (a) process has the process of changing said analysis object log file into a predetermined format, using a conversion procedure beforehand prepared for every application with this another invention which outputted said analysis object log file. As for this method, it is preferred to have further the process of updating a conversion procedure beforehand prepared for said every application to predetermined timing.

[0012]By using a procedure beforehand prepared for every analysis object log file, it becomes possible to analyze a log efficiently. It becomes possible by updating this procedure suitably to raise accuracy of log analysis.

[0013]According to further another embodiment of 1, it has further the process of classifying a line belonging to the same session from said analysis object log before the (e) aforementioned (a) process or the (b) process. In this case, as for the aforementioned (e) process, it is preferred among an analysis object log that it is what distinguishes to which session a line which cannot distinguish that session that belongs belongs based on a line which can distinguish that session that belongs.

[0014]According to such composition, apparently, even if it belongs to which session or is an unknown line, it becomes possible to classify at a suitable session. Therefore, it is effective in the ability to conduct next log analysis efficiently and effectively.

[0015]The aforementioned (b) process is further another thing that will unify said two or more analysis object logs for every same session if it depends like 1 operative condition. In this case, the aforementioned (c) process distinguishes existence of unlawful access for every analysis object log integrated for said every same session. In this case, as for the aforementioned (c) process, it is desirable that it is what classifies by color and displays the possibility of unlawful access for said every session.

[0016]According to such composition, by summarizing each log for every session at the time of log integration, unlawful access can be distinguished effectively and a display of the result becomes easy.

[0017]A means which according to the 2nd main viewpoint of this invention carries out the conversion process of each analysis object log file which application which can record a communication log of (a) plurality outputted to a predetermined format when required, (b) A communication log processing system having a means to unify two or more analysis object logs changed into said predetermined format, and a means to judge existence of unlawful access by analyzing a log after (c) integration was carried out is provided.

[0018]According to such composition, a system which can perform a method concerning said 1st viewpoint can be obtained.

[0019]According to the 3rd main viewpoint of this invention, are the computer software program products which collaborate with operation system installed in a computer system, and perform analysis processing of

Computer software program products having a means to judge existence of unlawful access by being stored in said storage and analyzing a log after being unified are provided.

[0020]According to such composition, the same effect as a method concerning main viewpoints of the above 1st can be acquired.

[0021]Other features of this invention and a prominent effect are more clearly understood by referring to a paragraph and an attached drawing of an embodiment of the next invention.

[0022]

[Embodiment of the Invention]Hereafter, an embodiment of the invention is described based on a drawing.

[0023]First, it is a server of a surveillance object which that one shows shows by the log analyzing system of this embodiment, and 2 among drawing 1. The log analyzing system 1 of this embodiment does so the function to receive and analyze on-line the communication log which said server 2 outputted, in order to discover unlawful access from a cracker, for example.

[0024]That is, in said server 2, the record and the output of the communications processing of the various server applications 3 are done using the log record program 4. And the log transport agent 5 similarly installed in this server 2 transmits said communication log to said log analyzing system 1 in real time through LAN, a public line, and other communications networks. This log analyzing system 1 is stored in the analysis object log storage 7 in which the received communication log was provided by this log analyzing system 1.

[0025]Taking out and analyzing the communication log stored in said analysis object log storage 7 to predetermined timing searches for the existence of unlawful access in said log analyzing system 1 (process shown in drawing 1 by 8). and the analysis result is outputted for example, in list form -- it is like (process shown in drawing 1 by 9).

[0026]The log analyzing system 1 of this invention carries out the integrating process of the various communication logs. In order to correspond to this, in the server 2 of this embodiment, the same event is recorded on two or more log files, and it transmits to this log analyzing system 1. Drawing 2 (a) and (b) shows the example of the record method of such a communication log.

[0027]As shown in drawing 2 (a) in this case, said server 2 Namely, two or more server applications A about the same event. As the communication log of B may be recorded on different communications log file A using two or more log record programs 4A and 4B, and B and it is shown in drawing 2 (b), The communication log of two or more applications A and B may be recorded on different communications log file A using the single log record program 4A, and B.

[0028]In this case, as for said two or more log files, it is preferred that it is a different thing prepared for every facility. For example, in this embodiment, the communication log for every facility is recorded on "/var/log / facility name .log" about the same event. In this embodiment, the communication log of all the facility about the same event is recorded on one file "/var / log/all.log" for the reference consistency with the communications log file for every above-mentioned facility.

[0029]Next, with reference to drawing 3, the log analyzing system 1 of this embodiment is explained

the analysis performed with this analyzing system besides said analysis object log storage 7, The unification log storage 21 which stores the log after the format was unified, the unified analysis object log storage 22 which stores the analysis object log integrated, and the analysis result storage 23 which stores the analysis result of a log are formed.

[0032]The updated default analysis condition file 24a which security contractors, such as an applicant of this application, provide, and the user setting-out analysis condition file 24b which the user of this system set up based on this default analysis condition file are stored in said analysis condition storage 19.

[0033]If the thing only related to this invention is mentioned to the program storing part 16, The analysis condition set part 25 for setting up the terms and conditions of said analysis, and the log format conversion treating part 26 which carries out the conversion process of said analysis object log file to a predetermined unified format, and stores it in said unification log storage 21 so that comparison or combination with mutual may be possible, The compatibility discrimination section 27 which distinguishes the compatibility between two or more analysis object logs, and the log integration processing part 28 which unifies two or more analysis object logs changed into said predetermined format, The log sorting process part 29 which classifies the line which belongs to the same facility from said analysis object log integrated, It has the log analysis processing part 30 which judges the existence of unlawful access by analyzing said classified analysis object log, and the analysis result reflection treating part 36 for making the analysis result by this log analysis processing part 30 reflect in said analysis setting out.

[0034]The log integration processing part 28 has the session discrimination section 31 which distinguishes whether it is classified at which session about the line which cannot distinguish a session based on the line which can be classified among an analysis object log.

[0035]The log analysis processing part 30 is provided with the following.

Connection IP analyzor 33 which judges unlawful access based on a connection IP address.

Connect time analyzor 34 which judges unlawful access based on connect time.

Pattern analyzor 35 which judges the existence of unlawful access by comparing with the connection pattern which prepared said log beforehand.

[0036]These components are the programs actually installed in the fixed field secured to the storage of the computer system, and this field, and it is that are called by said CPU11 on RAM12 and it performs, It collaborates with OS (operation system) and the function of this invention is done so.

[0037]Hereafter, the function and operation of the above-mentioned component are explained with the procedure of this system.

[0038]Drawing 3 shows the procedure of the outline by this analyzing system 1.

[0039]As shown in this figure, analysis of the communication log using this analyzing system 1 is conducted by wizard form, for example. When a wizard is started (Step S1), said analysis condition set part 25 makes an analysis condition set up at Steps S2-S6 first. Setting out of this analysis condition Setting out of setting

operator which is not detailed setting Steps S3-S6 as network security, and in this embodiment. As shown in drawing 5, "Regulation" which is setting out which is effective now "Web general relation" 40 which analyze unlawful access related to 38, "basic setting-out" 39 for conducting unlawful access analysis generally, and other WEB(s) of CGI, "ftp motion analysis" 41 which check the item related to Ftp, and manager authority. "root access analysis" 42 which have and analyze the record which operated, "scan motion analysis" 43 which analyze the housekeeping operation before receiving unlawful access, and the "mailing environment analysis" 44 grade which analyzes the abnormal operation of mailing environment can be chosen now. By choosing each setting out, the analytical item etc. by which default configuration was carried out about each setting out so that it might mention later can set up now automatically. Therefore, an operator may only correct these.

[0041]In this embodiment, said security policies other than the above "regulation" can be set up now using the newest updated default analysis condition file 24a that security contractors, such as an applicant of this application, prepared. Therefore, when choosing choices other than the above "regulation", the operator can use the newest security policy, without being conscious.

[0042]Next, in setting out (Step S3) of permission IP and refusal IP, IP (permission IP) which permits access for every facility, and IP (refusal IP) which refuses access can be set up now. Refusal IP which said security contractor added to said updated default analysis condition file 24a in this embodiment, Refusal IP which said analysis result reflection treating part 36 judged to be suitable as a result of the security diagnosis of this system is automatically displayed as a default based on the above selected policy.

[0043]The pattern which should be supervised for every facility can be set up now in pattern setting out (step S4). For example, in APP, the pattern which should be supervised about a boot force attack, port scan, etc. can be set up now. The newest thing is always provided as a default by said default analysis condition file 24a provided also with such a pattern by said security contractor according to each policy. For this reason, the operator can perform optimal setting out, if a default pattern is applied fundamentally.

[0044]next, an analysis object file — choosing (Step S5) — in this example, the file the directory set up as said analysis object log storage 7 and in that directory can be individually specified now.

[0045]In selection of an analytical item, and selection (Step S6) of a report output kind, connection IP analysis, connect time analysis, and pattern analysis can be chosen now as an analytical item corresponding to said each connection IP analyzor 33, the connect time analyzor 34, and the pattern analyzor 35. In a report output item, when displaying the item which should be outputted in a report, for example, said communication log, it can be specified whether items, such as time and a facility name, are displayed.

[0046]The item set up above is stored in the user setting-out analysis condition 24b of said analysis condition storage 19, and analysis succeedingly shown in drawing 4 at Step S7 is performed.

[0047]Hereafter, this procedure is explained based on the flow chart of drawing 6.

[0048]First, said format conversion treating part 26 takes out the analysis object communication log set up by said analysis condition, carries out a conversion process to a predetermined format, and stores the

(xferlog) that recorded movement of the file in ftp presupposes that it is what is shown in drawing 7 (b). Here the 1st log to being the form {the moon, a day, time, a server, a demon, and [PID] operation (connection IP and account are included)} the 2nd log, It is the form {a day of the week, the moon, a day, time, a year, connection IP, a file size, a file name, transfer mode, input and output, account, and a protocol}. The way things stand, even if it performs the integrating process explained later, it becomes like drawing 8, and since that analysis is difficult, said format conversion treating part 26 arranges these with a form as shown in drawing 9 at this embodiment. In this form, the form of the time stamp of the form of drawing 7 (a) and drawing 7 (b) is doubled, and the display position of connection IP and the display position of account are arranged.

[0050]Subsequently, said compatibility discrimination section 27 distinguishes the compatibility between the logs about the same event stored in said unification log storage 21 (step S7-2).

[0051]For example, all the logs (/var/log/all.log) recorded about operation of ftp as the same event show drawing 10 (a), and the log (/var/log/auth.log) about attestation presupposes that it is what is shown in drawing 10 (b). Here, the form of drawing 10 (a) is the thing before being {the moon, a day, time, a server, a demon (or service), and [PID] operation (connection IP and account are included)} and performing account format unification of the expedient kickback of explanation. In this case, if the log of drawing 10 (b) is applied to description of the log of drawing 10 (a), respectively, it will become 9 and the 16 or 17th line.

[0052]Said compatibility discrimination section 27 starts said all the logs by the most suitable method according to the kind of said log record program 4, and compares them with the log for every facility. In this example, all the logs of said drawing 10 (a) are started by using a "demon name" as a key, and it compares with said drawing 10 (b). As a result, when both are not in agreement, it can be judged that one of logs were altered. Here, all the logs are started by a demon name because said demon name (or service name) is being fixed for every facility. On the other hand, description of the same PID will be distributed by two or more logs in the record according to facility, and PID (process ID) is not preferred.

[0053]Since such optimal method of starting changes with forms of a log, it is made to perform this process (step S7-2) after said form unification process (step S7-1) actually in this embodiment. It becomes possible to perform said comparison consistency by a fixed method by this.

[0054]Next, said log integration processing part 28 unifies two or more analysis object logs changed into said predetermined format (step S7-3). It is because unifying may not understand the existence of an unjust attack from each log file here.

[0055]For example, the 1st log (/var/log/info.log) shows drawing 11 (a) among the system logs (syslog) about the same event, and the case where the 2nd log (/var/log/auth.log) is what is shown in drawing 11 (b) is considered. In this case, the ftp session of session PID [2425] has doubt of unlawful access. However, as long as the 1st log is seen, the relation with PID [2425] carried out clearly does not understand even it by the grade by which the trace remains in the 3 times input of PID [2421] slightly. Conversely, the 2nd log understands clearly that record of failure of PID [2421] remains and p51-dp09 *** ne.jp is devising the Bluto

means is the Bluto force attack to ftp using Telnet.

[0057]Such analysis cannot be obtained from each log of drawing 11 (a) and drawing 11 (b). Therefore, it is necessary to combine and analyze these two logs.

[0058]Hereafter, the log coupling method of this embodiment is explained.

[0059]After this log integration processing part 28 unifies the format of each log at the format unification process mentioned above, it combines these and obtains the log combined like drawing 9. That is, as mentioned above, about ftp, operation of itself and movement of a file are recorded on a separate log file (drawing 8 (a) and drawing 8 (b)). Since formats differ, these two logs are difficult to conduct the analysis, if it joined together simply. For this reason, these are combined after unifying by the method which mentioned the form of two logs above.

[0060]However, in such an example, it becomes a problem that there is no description which specifies operation of ftp as the log of drawing 8 (b). In the example of drawing 8 and drawing 9, since there is only one ftp, the specification is easy, but since the specification cannot be performed for example, when the identical time range has two or more ftp sessions, effective analysis can be conducted.

[0061]For this reason, in this embodiment, processing which distributes the line the session of whose which distinguishes and belongs [to which session each line of a log file belongs and] is unknown at the above-mentioned log integration processing part 28 to a suitable session is performed.

[0062]The example of the 1st log (syslog) in case drawing 13 (a) has two or more sessions in the time range, and drawing 13 (b) are the examples of the 2nd log (xferlog). The arranging [unified these two logs by this log integration processing part 28, and]-in order of time stamp-them thing after unifying a format like the above by said log format conversion treating part 26 is drawing 14.

[0063]In the unified log of this drawing 14, it is quite difficult to analyze, since there is a session which overlaps with identical time or there is a session from the same IP.

[0064]For this reason, in this log integration processing part 28, the attribute of a session is distinguished first (step S7-4). In this case, when the log of said drawing 13 (a) is divided for every PID, and the line which can be judged to be the same session is classified, as it is shown in drawing 15 (a) - (c), it turns out that three sessions exist. Therefore, PID, IP, and the connect time of each session distinguish that it seems that it is shown in drawing 16 from this result (step S7-5).

[0065]The log of said drawing 13 (b) can be classified according to using this data at one of sessions, as shown in drawing 17 (a) - (c).

[0066]Said log integration processing part 28 arranges said drawing 15 and drawing 17 in order of a time stamp the whole session, and obtains the result of drawing 18 (a) - (c) (step S7-6). Such a unified log is stored in said unified analysis object log storage 22.

[0067]Subsequently, said classification distribution part 29 classifies said log integrated for every facility (step S7-7). According to this embodiment, the log stored in said unified analysis object log storage is taken out, and it distributes to a demon name (service name) paying attention to each line in a log.

[0069]First, detection processing of "permission IP" set up above or "refusal IP" is performed by the connection IP analysis processing of step S7-8. IP and the domain which were set as permission IP will be removed from other following analysis objects. Subsequently, IP which connection established among IP detected as IP or said refusal IP other than permission IP is detected, and the log about this IP is extracted.

[0070]Next, in the inaccurate connect time detection processing of step S7-9, the connection of those other than the time zone set up as a connect time belt is detected as inaccurate connect time, and the log concerning the inaccurate connect time concerned is extracted.

[0071]Next, in pattern analysis of step S7-10, coincidence with said log and the pattern stored in said analysis condition storage is judged, and when in agreement, it detects as unlawful access. As for this pattern, being updated every day is preferred, therefore the updated pattern is supplied by the security contractor as said updated default analysis condition file 24a in this embodiment. The number of the patterns used by this embodiment is about 400.

[0072]Finally, an analysis result is outputted at Step S8 of drawing 4. As for the output of this analysis result, it is preferred to be classified by color and displayed in red, yellow, etc., corresponding to the possibility of unlawful access. To each session, this analysis result sets the flag according to the possibility of unlawful access, and stores it in said analysis result storage 23.

[0073]The result of the analysis carried out in this way is reflected in said updated default analysis condition file 24a by said analysis result reflection treating part 36. For example, when there is IP judged to have accessed unlawfully as a result of said analysis, the IP concerned is stored in said default analysis condition file 24a as refusal IP.

[0074]According to such composition, the format of two or more log files is unified, and it becomes possible to detect unlawful access which cannot be distinguished with an independent log file by unifying them. Since a security contractor is carried out based on the newest format unification method and integrating method which were updated to predetermined timing, for example, these processes can discover unlawful access etc., without requiring advanced knowledge and experience of a security management person.

[0075]This invention is variously deformable in the range which is not limited to the one above-mentioned embodiment and does not change the gist of an invention.

[0076]For example, although the server 2 is made into a surveillance object, it is not limited to this, and it may be made to supervise a router etc. in said one embodiment.

[0077]At the one above-mentioned embodiment, although this invention was provided as a system and a method, it may do the function of this invention so by being provided as a software package stored in CD-ROM etc., and being installed in a computer system.

[0078]

[Effect of the Invention]According to the composition explained above, the log processing method and system which can discover unlawful access etc. can be obtained, without requiring advanced knowledge and experience of a security management person.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－318734
（P2002－318734A）
(43)公開日　平成14年10月31日(2002.10.31)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G06F	13/00	351	C06F	13/00	351N　5B042
	11/34			11/34	S　5B085
	15/00	320		15/00	320K　5B089
		330			330A

審査請求　未請求　請求項の数30　ＯＬ　（全 14 頁）

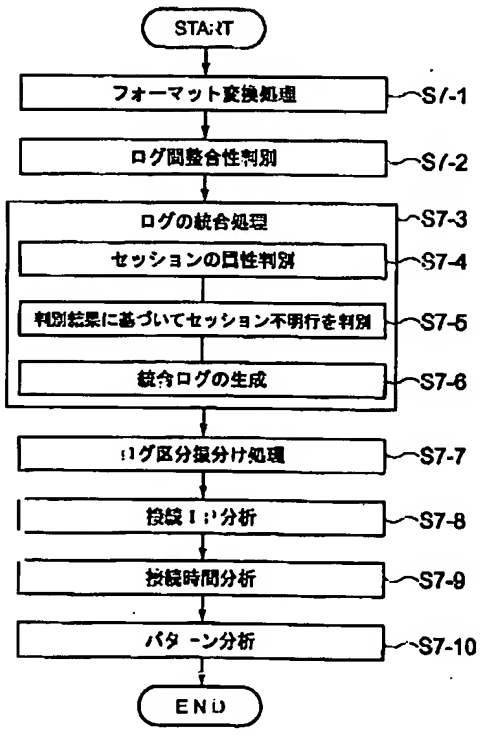
(21)出願番号　特願2001－120308(P2001－120308)
(22)出願日　平成13年４月18日(2001.4.18)

(71)出願人　501006882
株式会社チームガイア
東京都品川区上大崎３丁目14番37号
(72)発明者　阿部　ひろき
東京都品川区上大崎３丁目14番37号　株式会社チームガイア内
(74)代理人　100104215
弁理士　大森　純一　（外１名）

Ｆターム(参考)　5B042 GA12 GB09 MA14 MC40
5B085 AC11 AC14
5B089 GB02 KA17 KB13 KC29 KC32
KH04 MC01 MC03

(54)【発明の名称】　通信ログ処理方法及びシステム

(57)【要約】
【課題】　セキュリティ管理者に高度な知識や経験を要求することなく不正アクセス等を発見することができるログ処理方法及びシステムを提供する。
【解決手段】　（ａ）複数の通信ログを記録可能なアプリケーションが出力した各分析対象ログファイルを、必要な場合所定のフォーマットに変換処理する工程と、（ｂ）前記所定のフォーマットに変換された複数の分析対象ログを統合する工程と、（ｃ）統合された後のログを分析することで不正アクセスの有無を判断する工程とを有する。



【特許請求の範囲】
【請求項１】（ａ） 複数の通信ログを記録可能なアプリケーションが出力した各分析対象ログファイルを、必要な場合所定のフォーマットに変換処理する工程と、
（ｂ）前記所定のフォーマットに変換された複数の分析対象ログを統合する工程と、（ｃ）統合された後のログを分析することで不正アクセスの有無を判断する工程とを有することを特徴とする通信ログ処理方法
【請求項２】 請求項１記載の通信ログ処理方法において、
前記複数の分析対象ログファイルは、同一システムについて記録されたものであることを特徴とするログ通信処理方法。
【請求項３】 請求項２記載の通信ログ処理方法において、（ｄ）前記（ａ）工程若しくは（ｂ）工程の前に前記複数の分析対象ログ間の整合性を判別し、その判別結果を出力する工程をさらに有することを特徴とする通信ログ処理方法。
【請求項４】 請求項１記載の通信ログ処理方法において、
前記（ａ）工程は、前記分析対象ログファイルを出力したアプリケーション毎に予め用意された変換手順を利用して、前記分析対象ログファイルを所定のフォーマットに変換する工程を有するものであることを特徴とする通信ログ処理方法。
【請求項５】 請求項１記載の通信ログ処理方法において、
前記アプリケーション毎に予め用意された変換手順を、所定のタイミングで更新する工程をさらに有することを特徴とする通信ログ処理方法。
【請求項６】 請求項１記載の通信ログ処理方法において、
（ｅ）前記（ａ）工程若しくは（ｂ）工程の前に、前記分析対象ログから、同一セッションに属する行を分類する工程をさらに有することを特徴とする通信ログ処理方法。
【請求項７】 請求項６記載の通信ログ処理方法において、
前記（ｅ）工程は、分析対象ログ中、その属するセッションが判別できる行に基づいて、その属するセッションが判別できない行がどのセッションに属するかを判別する工程をさらに有することを特徴とする通信ログ処理方法。
【請求項８】 請求項１記載の通信ログ処理方法において、
前記（ｂ）工程は、前記複数の分析対象ログを同一セッション毎に統合するものであることを特徴とする通信ログ処理方法。
【請求項９】 請求項８記載の通信ログ処理方法において、
前記（ｃ）工程は、前記同一セッション毎に統合された分析対象ログ毎に、不正アクセスの有無を判別するものであることを特徴とする通信ログ処理方法。
【請求項１０】 請求項９記載の通信ログ処理方法において、
前記（ｃ）工程は、前記セッション毎に、不正アクセスの可能性を色分けして表示するものであることを特徴とする通信ログ処理方法。
【請求項１１】（ａ） 複数の通信ログを記録可能なアプリケーションが出力した各分析対象ログファイルを、必要な場合所定のフォーマットに変換処理する手段と、
（ｂ）前記所定のフォーマットに変換された複数の分析対象ログを統合する手段と、（ｃ）統合された後のログを分析することで不正アクセスの有無を判断する手段とを有することを特徴とする通信ログ処理システム。
【請求項１２】 請求項１１記載の通信ログ処理システムにおいて、
前記複数の分析対象ログファイルは、同一システムについて記録されたものであることを特徴とするログ通信処理システム。
【請求項１３】 請求項１２記載の通信ログ処理システムにおいて、
（ｄ）前記複数の分析対象ログ間の整合性を判別し、その判別結果を出力する手段をさらに有することを特徴とする通信ログ処理システム。
【請求項１４】 請求項１１記載の通信ログ処理システムにおいて、
前記（ａ）手段は、前記分析対象ログファイルを出力したアプリケーション毎に予め用意された変換手順を利用して、前記分析対象ログファイルを所定のフォーマットに変換する手段を有するものであることを特徴とする通信ログ処理システム。
【請求項１５】 請求項１１記載の通信ログ処理システムにおいて、
前記アプリケーション毎に予め用意された変換手順を、所定のタイミングで更新する手段をさらに有することを特徴とする通信ログ処理システム。
【請求項１６】 請求項１１記載の通信ログ処理システムにおいて、
（ｅ）前記分析対象ログから、同一セッションに属する行を分類する手段をさらに有することを特徴とする通信ログ処理システム。
【請求項１７】 請求項１６記載の通信ログ処理システムにおいて、
前記（ｅ）手段は、分析対象ログ中、その属するセッションが判別できる行に基づいて、その属するセッションが判別できない行がどのセッションに属するかを判別する手段をさらに有することを特徴とする通信ログ処理システム。
【請求項１８】 請求項１１記載の通信ログ処理システ

ムにおいて、
前記（ｂ）手段は、前記複数の分析対象ログを同一セッション毎に統合するものであることを特徴とする通信ログ処理システム。
【請求項１９】　請求項１８記載の通信ログ処理システムにおいて、
前記（ｃ）手段は、前記同一セッション毎に統合された分析対象ログ毎に、不正アクセスの有無を判別するものであることを特徴とする通信ログ処理システム。
【請求項２０】　請求項１９記載の通信ログ処理システムにおいて、
前記（ｃ）手段は、前記セッション毎に、不正アクセスの可能性を色分けして表示するものであることを特徴とする通信ログ処理システム。
【請求項２１】　コンピュータシステムにインストールされたオペレーションシステムと協働して通信ログの分析処理を行うコンピュータソフトウェアプログラム製品であって、
記憶媒体と、（ａ）この記憶媒体に格納され、複数の通信ログを記録可能なアプリケーションが出力した各分析対象ログファイルを、必要な場合所定のフォーマットに変換処理する手段と、（ｂ）前記記憶媒体に格納され、前記所定のフォーマットに変換された複数の分析対象ログを統合する手段と、（ｃ）前記記憶媒体に格納され、統合された後のログを分析することで不正アクセスの有無を判断する手段とを有することを特徴とするコンピュータソフトウェアプログラム製品。
【請求項２２】　請求項２１記載のコンピュータソフトウェアプログラム製品において、前記複数の分析対象ログファイルは、同一システムについて記録されたものであることを特徴とするログ通信処理システム。
【請求項２３】　請求項２２記載のコンピュータソフトウェアプログラム製品において、
（ｄ）前記記憶媒体に格納され、前記複数の分析対象ログ間の整合性を判別し、その判別結果を出力する手段をさらに有することを特徴とするコンピュータソフトウェアプログラム製品。
【請求項２４】　請求項２１記載のコンピュータソフトウェアプログラム製品において、
前記（ａ）手段は、前記分析対象ログファイルを出力したアプリケーション毎に予め用意された変換手順を利用して、前記分析対象ログファイルを所定のフォーマットに変換する手段を有するものであることを特徴とするコンピュータソフトウェアプログラム製品。
【請求項２５】　請求項２１記載のコンピュータソフトウェアプログラム製品において、
前記アプリケーション毎に予め用意された変換手順を、所定のタイミングで更新する手段をさらに有することを特徴とするコンピュータソフトウェアプログラム製品。
【請求項２６】　請求項２１記載のコンピュータソフトウェアプログラム製品において、（ｅ）前記記憶媒体に格納され、前記分析対象ログから、同一セッションに属する行を分類する手段をさらに有することを特徴とするコンピュータソフトウェアプログラム製品。
【請求項２７】　請求項２６記載のコンピュータソフトウェアプログラム製品において、
前記（ｅ）手段は、分析対象ログ中、その属するセッションが判別できる行に基づいて、その属するセッションが判別できない行がどのセッションに属するかを判別する手段をさらに有することを特徴とするコンピュータソフトウェアプログラム製品。
【請求項２８】　請求項２１記載のコンピュータソフトウェアプログラム製品において、
前記（ｂ）手段は、前記複数の分析対象ログを同一セッション毎に統合するものであることを特徴とするコンピュータソフトウェアプログラム製品。
【請求項２９】　請求項２８記載のコンピュータソフトウェアプログラム製品において、
前記（ｃ）手段は、前記同一セッション毎に統合された分析対象ログ毎に、不正アクセスの有無を判別するものであることを特徴とするコンピュータソフトウェアプログラム製品。
【請求項３０】　請求項２９記載のコンピュータソフトウェアプログラム製品において、
前記（ｃ）手段は、前記セッション毎に、不正アクセスの可能性を色分けして表示するものであることを特徴とするコンピュータソフトウェアプログラム製品。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、通信サーバで記録された通信ログを分析するための通信ログ処理方法及びそのシステム等に関するものであり、特に、複数のログ出力が可能なアプリケーションから出力された通信ログを統一的に分析できる方法等に関するものである。
【０００２】
【従来の技術】最近、クラッカー等により企業や官公庁のネットワークやサーバが攻撃されるという事件が多発している。このことにより、ネットワークセキュリティの強化に注目が集まっている。ネットワークセキュリティを強化するには、まず、ネットワークのセキュリティを監視・分析する必要がある。ネットワークセキュリティの監視には、ネットワークを構成するサーバ等の装置の通信ログを記録し分析することが有効である。
【０００３】この通信ログは、サーバ等の通信履歴が記録されたものであり、これを分析することで、このサーバに起こった全ての事象が検出できる。例えば 外部から前記サーバに対して不自然なアクセスがあったことに基づいて不正アクセスがあったことを検知できる。従って、これに応じて何らかの対策を立てることで、ネットワークのセキュリティを強化することができる。

【0004】
【発明が解決しようとする課題】しかしながら、通常サーバから出力されるログは、コンピュータのOSや使用されているアプリケーションによってそれぞれ異なったフォーマットで記録されており、多種多様である。また、その量があまりにも膨大であるため、内容をチェックすることができないかチェックするための時間が確保できないという、システム管理上問題のある状態でネットワークが運用されているのが一般的である。
【0005】また、ネットワークに対して攻撃を仕掛けるクラッカーは、自己のネットワーク進入の形跡を消去するために前記ログを改竄若しくは削除することもあり、この場合には、このような不正アクセスを発見することは極めて困難である。
【0006】この発明は、このような事情に鑑みてなされたものであり、セキュリティ管理者に高度な知識や経験を要求することなく不正アクセス等を発見することができるログ処理方法及びシステムを提供することを目的とする。
【0007】
【課題を解決するための手段】上記課題を解決するため、この発明の第1の主要な観点によれば、（a）複数の通信ログを記録可能なアプリケーションが出力した各分析対象ログファイルを、必要な場合所定のフォーマットに変換処理する工程と、（b）前記所定のフォーマットに変換された複数の分析対象ログを統合する工程と、（c）統合された後のログを分析することで不正アクセスの有無を判断する工程とを有することを特徴とする通信ログ処理方法が提供される。
【0008】このような構成によれば、複数のログファイルのフォーマットを、ログファイル毎に定められた方法で統一し、それらを統合することで、単独のログファイルでは判別することができない不正アクセスを検出することが可能になる。
【0009】ここで、この発明の1の実施態様によれば、前記複数の分析対象ログファイルは、同一システムについて記録されたものであることが好ましい。また、この場合、この方法はさらに、（d）前記（a）工程若しくは（b）工程の前に前記複数の分析対象ログ間の整合性を判別し、その判別結果を出力する工程を有することが好ましい。
【0010】このような構成によれば、同一システム（ミラーリングサーバ含む）についてのログを複数のログファイルに記録してなるものを対象とした場合に、これらを統合することで、当該システムにおけるイベントが不正アクセスを含むものであるかを判別することができる。また、複数のファイル間の整合性を判別することで、一部のファイルが改竄等されたことを検出することができる。
【0011】また、この発明の別の1実施態様によれば、前記（a）工程は、前記分析対象ログファイルを出力したアプリケーション毎に予め用意された変換手順を利用して、前記分析対象ログファイルを所定のフォーマットに変換する工程を有するものである。また、この方法は、前記アプリケーション毎に予め用意された変換手順を、所定のタイミングで更新する工程をさらに有することが好ましい。
【0012】分析対象ログファイル毎に予め用意された手順を利用することで、ログの分析を効率的に行うことが可能になる。また、この手順を適宜更新することで、ログ分析の精度を向上させることが可能になる。
【0013】更なる別の1の実施態様によれば、（e）前記（a）工程若しくは（b）工程の前に、前記分析対象ログから、同一セッションに属する行を分類する工程をさらに有する。この場合、前記（e）工程は、分析対象ログ中、その属するセッションが判別できる行に基づいて、その属するセッションが判別できない行がどのセッションに属するかを判別するものであることが好ましい。
【0014】このような構成によれば、一見、どのセッションに属するか不明の行であっても、適切なセッションに分類することが可能になる。したがって、後のログ分析を効率的かつ効果的に行える効果がある。
【0015】更なる別の1実施態様によれば、前記（b）工程は、前記複数の分析対象ログを同一セッション毎に統合するものである。この場合、前記（c）工程は、前記同一セッション毎に統合された分析対象ログ毎に、不正アクセスの有無を判別するものである。この場合、前記（c）工程は、前記セッション毎に、不正アクセスの可能性を色分けして表示するものであることが望ましい。
【0016】このような構成によれば、ログ統合時に各ログをセッション毎に纏めることで、不正アクセスの判別を効果的に行え、その結果の表示が容易になる。
【0017】また、この発明の第2の主要な観点によれば、（a）複数の通信ログを記録可能なアプリケーションが出力した各分析対象ログファイルを、必要な場合所定のフォーマットに変換処理する手段と、（b）前記所定のフォーマットに変換された複数の分析対象ログを統合する手段と、（c）統合された後のログを分析することで不正アクセスの有無を判断する手段とを有することを特徴とする通信ログ処理システムが提供される。
【0018】このような構成によれば、前記第1の観点に係る方法を実行することができるシステムを得ることができる。
【0019】さらに、この発明の第3の主要な観点によれば、コンピュータシステムにインストールされたオペレーションシステムと協働して通信ログの分析処理を行うコンピュータソフトウェアプログラム製品であって、記憶媒体と、（a）この記憶媒体に格納され、複数の通

信ログを記録可能なアプリケーションが出力した各分析対象ログファイルを、必要な場合所定のフォーマットに変換処理する手段と、（ｂ）前記記憶媒体に格納され、前記所定のフォーマットに変換された複数の分析対象ログを統合する手段と、（ｃ）前記記憶媒体に格納され、統合された後のログを分析することで不正アクセスの有無を判断する手段とを有することを特徴とするコンピュータソフトウェアプログラム製品が提供される。

【００２０】このような構成によれば、上記第１の主要な観点にかかる方法と同様の効果を得ることができる。

【００２１】なお、この発明の他の特徴と顕著な効果は次の発明の実施形態の項及び添付した図面を参照することによって、より明確に理解される。

【００２２】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づき説明する。

【００２３】まず、図１中、１で示すのがこの実施形態のログ分析システム、２で示すのは監視対象のサーバである。この実施形態のログ分析システム１は、例えばクラッカーからの不正アクセスを発見するために、前記サーバ２が出力した通信ログをオンラインで受け取って分析する機能を奏するものである。

【００２４】すなわち、前記サーバ２では、各種サーバアプリケーション３の通信処理を、ログ記録プログラム４を利用して記録・出力するようになっている。そして、同じくこのサーバ２にインストールされたログ転送プログラム５が、前記通信ログをＬＡＮ、公衆回線その他の通信網を通じて前記ログ分析システム１にリアルタイムで転送する。このログ分析システム１は、受け取った通信ログを、このログ分析システム１に設けられた分析対象ログ格納部７に格納するようになっている。

【００２５】前記ログ分析システム１では、所定のタイミングで前記分析対象ログ格納部７に格納された通信ログを取り出して分析することで、不正アクセスの有無を探索する（図１に８で示す工程）。そして、その分析結果を例えば一覧形式で出力する（図１に９で示す工程）ようになっている。

【００２６】また、この発明のログ分析システム１は、多種多様な通信ログを統合処理することを特徴とするものである。これに対応するため、この実施形態のサーバ２では、同一のイベントを複数のログファイルに記録して、このログ分析システム１に転送するようになっている。図２（ａ）、（ｂ）は、このような通信ログの記録方法の例を示したものである。

【００２７】すなわち、この場合、前記サーバ２は、図２（ａ）に示すように、同一イベントについての複数のサーバアプリケーションＡ、Ｂの通信ログを、複数のログ記録プログラム４Ａ、４Ｂを利用して異なる通信ログファイルＡ、Ｂに記録しても良いし、図２（ｂ）に示すように、複数のアプリケーションＡ、Ｂの通信ログを、単一のログ記録プログラム４Ａを利用して異なる通信ログファイルＡ、Ｂに記録しても良い。

【００２８】この場合、前記複数のログファイルは、異なるファシリティ毎に用意されるものであることが好ましい。例えば、この実施形態では、同一のイベントについて各ファシリティ毎の通信ログを「/var/log/ファシリティ名.log」に記録する。また、この実施形態では、上記各ファシリティ毎の通信ログファイルとの参照整合用に、同一イベントについての全てのファシリティの通信ログを１つのファイル「/var/log/all.log」にも記録する。

【００２９】次に、図３を参照して、この実施形態のログ分析システム１について説明する。

【００３０】このシステムは、この図３に示すように、ＣＰＵ１１、ＲＡＭ１２、通信デバイス１３、その他の入出力デバイス１４等が接続されてなるバス１５に、プログラム格納部１６及びデータ格納部１７が接続されてなる。

【００３１】データ格納部１７には、前記分析対象ログ格納部７の他、この分析システムで実行する分析の諸条件を格納する分析条件格納部１９と、フォーマットが統一された後のログを格納する統一ログ格納部２１と、統合された分析対象ログを格納する統合済み分析対象ログ格納部２２と、ログの分析結果を格納する分析結果格納部２３とが設けられている。

【００３２】なお、前記分析条件格納部１９には、本出願の出願人等のセキュリティ業者が提供する更新済みデフォルト分析条件ファイル２４ａと、このデフォルト分析条件ファイルに基づいてこのシステムの利用者が設定した利用者設定分析条件ファイル２４ｂとが格納されている。

【００３３】また、プログラム格納部１６には、この発明にのみ関係するものを挙げると、前記分析の諸条件を設定するための分析条件設定部２５と、前記分析対象ログファイルを相互に比較若しくは結合可能なように所定の統一フォーマットに変換処理して前記統一ログ格納部２１に格納するログフォーマット変換処理部２６と、複数の分析対象ログ間の整合性を判別する整合性判別部２７と、前記所定のフォーマットに変換された複数の分析対象ログを統合するログ統合処理部２８と、前記統合された分析対象ログから同一ファシリティに属する行を区分するログ区分処理部２９と、前記区分された分析対象ログを分析することで不正アクセスの有無を判断するログ分析処理部３０と、このログ分析処理部３０による分析結果を前記分析設定に反映させるための分析結果反映処理部３６とを有する。

【００３４】なお、ログ統合処理部２８は、分析対象ログ中、セッションが判別できない行について、分類可能な行に基づいて、どのセッションに分類されるかを判別するセッション判別部３１を有する。

【００３５】また、ログ分析処理部３０は、接続ＩＰアドレスに基づいて不正アクセスを判断する接続ＩＰ分析部３３と、接続時間に基づいて不正アクセスを判断する接続時間分析部３４と、前記ログを予め用意した接続パターンと比較することで不正アクセスの有無を判断するパターン分析部３５とを有する。

【００３６】これらの構成要素は、実際にはコンピュータシステムの記憶媒体に確保された一定の領域及びこの領域にインストールされたプログラムであり、前記ＣＰＵ１１によってＲＡＭ１２上に呼び出されて実行されることで、ＯＳ（オペレーションシステム）と協働してこの発明の機能を奏するようになっている。

【００３７】以下、上記構成要素の機能及び動作をこのシステムの処理手順と共に説明する。

【００３８】図３は、この分析システム１による概略の処理手順を示したものである。

【００３９】この図に示すように、この分析システム１を利用した通信ログの分析は、例えば、ウィザード形式によって行われる。ウィザードを開始すると（ステップＳ１）、まず、前記分析条件設定部２５がステップＳ２～Ｓ６で分析条件の設定を行わせる。この分析条件の設定は、分析ポリシーの設定（ステップＳ２）、許可ＩＰ及び拒否ＩＰの設定（ステップＳ３）、パターン設定（ステップＳ４）、分析対象ファイル選択（ステップＳ５）、分析項目の選択及びレポート出力種類の選択（ステップＳ６）の順に実行されていくことが好ましい。

【００４０】ここで、前記分析ポリシーの設定（ステップＳ２）は、ネットワークセキュリティに詳しくないオペレータがステップＳ３～Ｓ６の設定をする際の負担を軽くするためのものであり、この実施形態では、図５に示すように、現在有効になっている設定である「規定」３８、全般的に不正アクセス分析を行うための「基本設定」３９、ＣＧＩの他ＷＥＢに関係する不正アクセスを分析する「Ｗｅｂ関係一般」４０、Ｆｔｐに関係する項目をチェックする「ｆｔｐ動作分析」４１、管理者権限をもって動作した記録を分析する「ｒｏｏｔアクセス分析」４２、不正アクセスを受ける前の準備動作を分析する「ｓｃａｎ動作分析」４３、メール環境の異常動作を分析する「メール環境分析」４４等を選択できるようになっている。各設定を選択することで、後述するように各設定についてデフォルト設定された分析項目等が自動的に設定できるようになっている。したがって、オペレータはこれらを修正していくのみで良い。

【００４１】また、この実施形態では、この出願の出願人等のようなセキュリティ業者が用意した最新の更新済みデフォルト分析条件ファイル２４ａを利用して前記「規定」以外の前記セキュリティポリシーの設定が行えるようになっている。従って、前記「規定」以外の選択肢を選ぶ場合、オペレータは意識することなく、最新のセキュリティポリシーを利用することができるようになっている。

【００４２】次に、許可ＩＰ及び拒否ＩＰの設定（ステップＳ３）では、ファシリティ毎にアクセスを許可するＩＰ（許可ＩＰ）やアクセスを拒否するＩＰ（拒否ＩＰ）を設定できるようになっている。この実施形態では、前記セキュリティ業者が前記更新済みデフォルト分析条件ファイル２４ａに追加した拒否ＩＰや、前記分析結果反映処理部３６がこのシステムのセキュリティ診断の結果適当であると判断した拒否ＩＰが前記で選択したポリシーに基づいて自動的にデフォルトとして表示されるようになっている。

【００４３】パターン設定（ステップＳ４）では、ファシリティ毎に監視すべきパターンを設定できるようになっている。例えば、ＡＰＰでは、ブートフォースアタックやポートスキャン等について監視するべきパターンを設定できるようになっている。このようなパターンも、前記セキュリティ業者から提供された前記デフォルト分析条件ファイル２４ａによって常に最新のものが各ポリシーに応じてデフォルトとして提供されるようになっている。このため、オペレータは、基本的にデフォルトのパターンを適用すれば、最適の設定を行える。

【００４４】次に、分析対象ファイルを選択する（ステップＳ５）が、この例では、前記分析対象ログ格納部７として設定されたディレクトリ及びそのディレクトリ内のファイルを個別に指定することができるようになっている。

【００４５】また、分析項目の選択及びレポート出力種類の選択（ステップＳ６）では、分析項目として、前記各接続ＩＰ分析部３３、接続時間分析部３４及びパターン分析部３５に対応して、接続ＩＰ分析、接続時間分析及びパターン分析が選択できるようになっている。また、レポート出力項目では、レポートで出力するべき項目、例えば、前記通信ログを表示する際に、時刻、ファシリティ名等の項目を表示するか等を指定できるようになっている。

【００４６】以上で設定された項目は、前記分析条件格納部１９の利用者設定分析条件２４ｂに格納され、引き続いて図４にステップＳ７で示す分析が実行される。

【００４７】以下、この手順を図６のフローチャートに基づいて説明する。

【００４８】まず、前記フォーマット変換処理部２６が、前記分析条件で設定した分析対象通信ログを取り出し、所定のフォーマットに変換処理し、変換処理後の通信ログを前記統一ログ格納部２１に格納する（ステップＳ７－１）。このフォーマット変換は、例えば、表示位置、表示順序、タイムスタンプの位置等、対象ファシリティやログ記録プログラムによって異なるフォーマットを統一フォーマットに揃えるものである。

【００４９】例えば、ｆｔｐの動作を記録した第１のログ（syslog）が図７（ａ）に示すものであり、ｆｔｐに

おけるファイルの移動を記録した第２のログ（xferlog）が図７（ｂ）に示すものであるとする。ここで、第１のログは、{月、日、時間、サーバ、デーモン、［ＰＩＤ］動作（接続ＩＰ、アカウントを含む）}という書式であるのに対して、第２のログは、{曜日、月、日、時間、年、接続ＩＰ、ファイルサイズ、ファイル名、転送モード、入出力、アカウント、プロトコル}という書式になっている。このままでは、後で説明する統合処理を行ったとしても、図８のようになりその分析が困難であるため、この実施形態では、前記フォーマット変換処理部２６が、これらを、図９に示すような書式に揃える。この書式では、図７（ａ）と図７（ｂ）の書式のタイムスタンプの書式を合わせ、接続ＩＰの表示位置とアカウントの表示位置が揃えられている。

【００５０】ついで、前記整合性判別部２７が、前記統一ログ格納部２１に格納された同一イベントについてのログ間の整合性を判別する（ステップＳ７－２）。

【００５１】例えば、同一イベントとして、ｆｔｐの動作に関して記録された全ログ（/var/log/all.log）が図１０（ａ）に示すものであり、認証に関するログ（/var/log/auth.log）が図１０（ｂ）に示すものであるとする。ここで、図１０（ａ）の書式は、{月、日、時間、サーバ、デーモン（若しくはサービス）、［ＰＩＤ］動作（接続ＩＰ、アカウントを含む）}となっており、説明の便宜上前記フォーマット統一を行う前のものである。この場合、図１０（ｂ）のログをそれぞれ図１０（ａ）のログの記述に当てはめると、９，１６，１７行目になる。

【００５２】前記整合性判別部２７は、前記全ログを、前記ログ記録プログラム４の種類に応じて最も適切な方法で切り出してファシリティ毎のログと比較する。この例では、「デーモン名」をキーとして前記図１０（ａ）の全ログを切り出して、前記図１０（ｂ）と比較する。この結果、両者が一致しない場合には、どちらかのログが改竄されたものと判断することができる。なお、ここで、デーモン名で全ログを切り出すのは、前記デーモン名（若しくはサービス名）は、ファシリティ毎に固定されているからである。一方ＰＩＤ（プロセスＩＤ）は、ファシリティ別の記録では同一ＰＩＤの記述が複数のログに分散されることになり好ましくない。

【００５３】このような最適な切り出し方法は、ログの書式によって異なるものであるから、この実施形態では、実際にはこの工程（ステップＳ７－２）を、前記書式統一工程（ステップＳ７－１）後に行うようにする。このことで、一定の方法で前記比較整合を行うことが可能になる。

【００５４】次に、前記ログ統合処理部２８が、前記所定のフォーマットに変換された複数の分析対象ログを統合する（ステップＳ７－３）。ここで、統合するのは、個々のログファイルからでは不正アタックの有無が分からない場合があるからである。

【００５５】例えば、同一イベントについてのシステムログ（syslog）のうち、第１のログ（/var/log/info.log）が図１１（ａ）に示すものであり、第２のログ（/var/log/auth.log）が図１１（ｂ）に示すものである場合について考える。この場合、セッションＰＩＤ［２４２５］のｆｔｐセッションは不正アクセスの疑いがある。しかし、第１のログを見る限りでは、その痕跡はＰＩＤ［２４２１］の３回入力にわずかに残る程度で、それさえもＰＩＤ［２４２５］とのはっきりとした関連は分からない。逆に第２のログには、ＰＩＤ［２４２１］の失敗の記録が残っていて、p51-dn09.***.ne.jpがブルートフォース（BruteForse）を仕掛けているのがはっきりと分かる。しかし、このログからではこのアタックが成功したかの判別はできない。また、このログにはＰＩＤ［２４２１］の表示はない。

【００５６】しかしながら、これらの動きは図１２に示す全ログ（/var/log/all.log）を見るとはっきりと現れている。すなわち、この一連のアタックは、2/16 15:09:04から始まっていて、手口はＴｅｌｎｅｔを利用したｆｔｐへのブルートフォースアタックであることが判る。

【００５７】このような分析は、図１１（ａ）、図１１（ｂ）の個々のログからは得ることができない。従って、この２つのログを結合して分析する必要があるのである。

【００５８】以下、この実施形態のログ結合方法について説明する。

【００５９】このログ統合処理部２８は、前述したフォーマット統一工程で各ログのフォーマットを統一した後、これらを結合し、図９のような結合済みのログを得る。すなわち、前述したように、例えば、ｆｔｐについては、それ自体の動作とファイルの移動とが別々のログファイル（図８（ａ）と図８（ｂ））に記録される。これら２つのログはフォーマットが異なるものであるから、単純に結合したのではその分析を行うことが困難である。このため、２つのログの書式を前述した方法で統一してからこれらを結合するのである。

【００６０】しかし、このような例において、問題になるのは、図８（ｂ）のログにｆｔｐの動作を特定する記述がないことである。図８及び図９の例では、ｆｔｐが一つしかないためその特定は容易であるが、例えば、同一時刻範囲に複数のｆｔｐセッションがある場合にはその特定ができないために、有効な分析が行えないことになる。

【００６１】このため、この実施形態では、上記ログ統合処理部２８で、ログファイルの各行がどのセッションに属するかを判別し、属するセッションが不明な行を適切なセッションに振分ける処理を行う。

【００６２】図１３（ａ）は同時刻範囲に複数のセッシ

ョンがある場合の第1のログ（syslog）の例、図１３（ｂ）は第2のログ（xferlog）の例である。この2つのログを前記ログフォーマット変換処理部２６で上記と同様にフォーマットを統一した後、このログ統合処理部２８で統合しタイムスタンプ順に並べたのものが図１４である。

【００６３】この図１４の統合済みログでは、同一時刻に重複しているセッションがあったり、同一ＩＰからのセッションがあったりするため解析するのはかなり困難である。

【００６４】このため、このログ統合処理部２８では、まず、セッションの属性を判別する（ステップＳ７－４）。この場合、前記図１３（ａ）のログをＰＩＤ毎に分け、同一セッションであると判断できる行を分類すると、図１５（ａ）～（ｃ）に示すように、３つのセッションが存在することがわかる。従って、この結果から、各セッションの、ＰＩＤ，ＩＰ及び接続時間は図１６に示すようであると判別する（ステップＳ７－５）。

【００６５】このデータを利用することで、前記図１３（ｂ）のログは、図１７（ａ）～（ｃ）に示すようにいずれかのセッションに分類できる。

【００６６】前記ログ統合処理部２８は、前記図１５及び図１７をセッション毎タイムスタンプ順に並べて、図１８（ａ）～（ｃ）の結果を得る（ステップＳ７－６）。このような統合済みログは前記統合済み分析対象ログ格納部２２内に格納される。

【００６７】ついで、前記区分振分け部２９が、前記統合されたログを、ファシリティ毎に区分する（ステップＳ７－７）。この実施形態では、前記統合済み分析対象ログ格納部に格納されたログを取り出し、ログ中の各行を、デーモン名（サービス名）に注目して振分けを行う。

【００６８】ついで、前記ログ分析処理部３０は、前記のように処理されたログファイルを利用して不正アクセスの有無の分析処理を実行する（ステップＳ７－８～Ｓ７－１０）。各ログは、前述したように、分析しやすいように纏められ区分されているため、以下の分析を効率的に行って行くことが可能になる。

【００６９】まず、ステップＳ７－８の接続ＩＰ分析処理で、前記で設定された「許可ＩＰ」若しくは「拒否ＩＰ」の検出処理を行う。許可ＩＰに設定されたＩＰ及びドメインは、以下の他の分析対象から外されることになる。ついで、許可ＩＰ以外のＩＰ若しくは前記拒否ＩＰとして検出されたＩＰのうち、接続が確立したＩＰを検出し、このＩＰに関するログを抽出する。

【００７０】次に、ステップＳ７－９の不正接続時間検出処理では、接続時間帯として設定された時間帯以外の接続を不正接続時間として検出し、当該不正接続時間に係るログを抽出する。

【００７１】次に、ステップＳ７－１０のパターン分析では、前記ログと前記分析条件格納部に格納されたパターンとの一致を判断し、一致した場合に不正アクセスとして検出する。このパターンは、日々更新されたものであることが好ましく、そのため、この実施形態では、更新されたパターンが前記更新済みデフォルト分析条件ファイル２４ａとしてセキュリティ業者から供給されるようになっている。この実施形態で用いるパターンは約４００種類である。

【００７２】最後に、図４のステップＳ８で分析結果を出力する。この分析結果の出力は、不正アクセスの可能性に応じて例えば、赤色や黄色等で色分けされて表示されることが好ましい。また、この分析結果は、各セッションに対して、不正アクセスの可能性に応じたフラグを立てて前記分析結果格納部２３に格納する。

【００７３】また、このように実施された分析の結果は、前記分析結果反映処理部３６によって前記更新済みデフォルト分析条件ファイル２４ａに反映される。例えば、前記分析の結果、不正アクセスを行ったと判断されたＩＰがある場合には、当該ＩＰは拒否ＩＰとして前記デフォルト分析条件ファイル２４ａに格納される。

【００７４】このような構成によれば、複数のログファイルのフォーマットを統一し、それらを統合することで、単独のログファイルでは判別することができない不正アクセスを検出することが可能になる。また、これらの工程は、例えばセキュリティ業者が所定のタイミングで更新した最新のフォーマット統一方法や統合方法に基づいて実施されるから、セキュリティ管理者に高度な知識や経験を要求することなく不正アクセス等を発見することができる。

【００７５】なお、この発明は、上記一実施形態に限定されるものではなく、発明の要旨を変更しない範囲で種々変形可能である。

【００７６】例えば、前記一実施形態ではサーバ２を監視対象としたがこれに限定されるものではなく、ルータ等を監視するようにしても良い。

【００７７】また、上記一実施形態では、この発明はシステム及び方法として提供されていたが、ＣＤ－ＲＯＭ等に格納されたパッケージソフトウェアとして提供されコンピュータシステムにインストールされることでこの発明の機能を奏するものであっても良い。

【００７８】

【発明の効果】以上説明した構成によれば、セキュリティ管理者に高度な知識や経験を要求することなく不正アクセス等を発見することができるログ処理方法及びシステムを得ることができる。

【図面の簡単な説明】

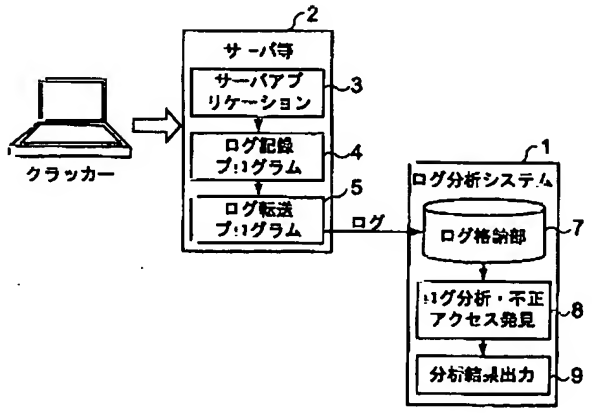
【図１】この発明の一実施形態を示す概略構成図。

【図２】この実施形態のログの記録方法を示す説明図。

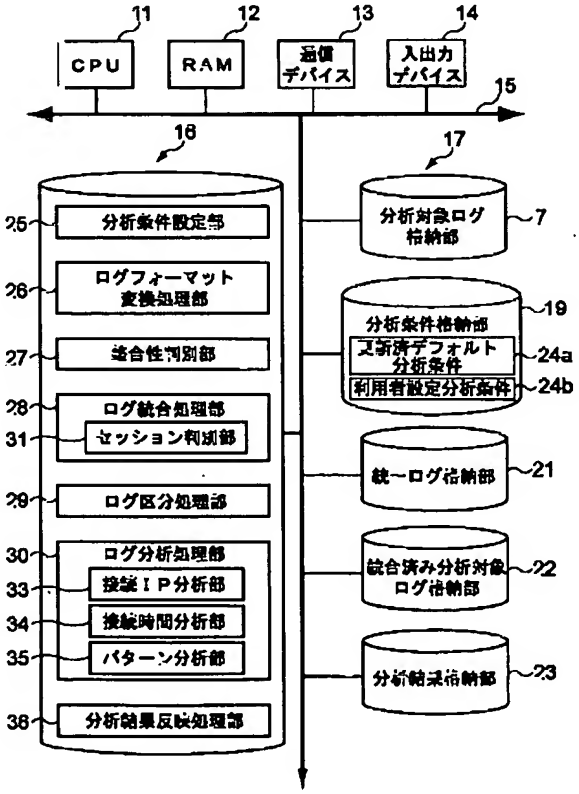
【図３】この実施形態のログ分析システムを示す概略構成図。

【図４】この実施形態の概略処理工程を示すフローチャート。
【図５】分析ポリシーの選択肢を説明する図。
【図６】分析処理の処理工程を示すフローチャート。
【図７】通信ログの処理例を示す図。
【図８】通信ログの処理例を示す図。
【図９】通信ログの処理例を示す図。
【図１０】通信ログの処理例を示す図。
【図１１】通信ログの処理例を示す図。
【図１２】通信ログの処理例を示す図。
【図１３】通信ログの処理例を示す図。
【図１４】通信ログの処理例を示す図。
【図１５】通信ログの処理例を示す図。
【図１６】通信ログの処理例を示す図。
【図１７】通信ログの処理例を示す図。
【図１８】通信ログの処理例を示す図。
【符号の説明】
1…ログ分析システム
2…サーバ
3…サーバアプリケーション
4…ログ記録プログラム
5…ログ転送プログラム
7…分析対象ログ格納部
11…ＣＰＵ
12…ＲＡＭ
13…通信デバイス
14…入出力デバイス
15…バス
16…プログラム格納部
17…データ格納部
19…分析条件格納部
21…統一ログ格納部
22…統合済み分析対象ログ格納部
23…分析結果格納部
24ａ…更新済みデフォルト分析条件ファイル
24ｂ…利用者設定分析条件ファイル
25…分析条件設定部
26…ログフォーマット変換処理部
27…整合性判別部
28…ログ統合処理部
29…ログ区分処理部
30…ログ分析処理部
31…セッション判別部
33…ＩＰ分析部
34…接続時間分析部
35…パターン分析部
36…分析結果反映処理部

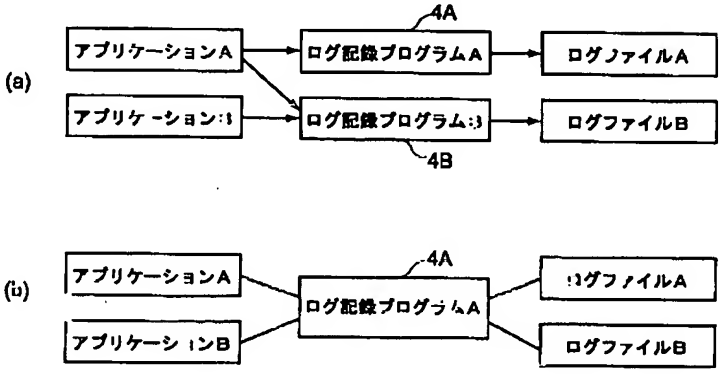
【図1】



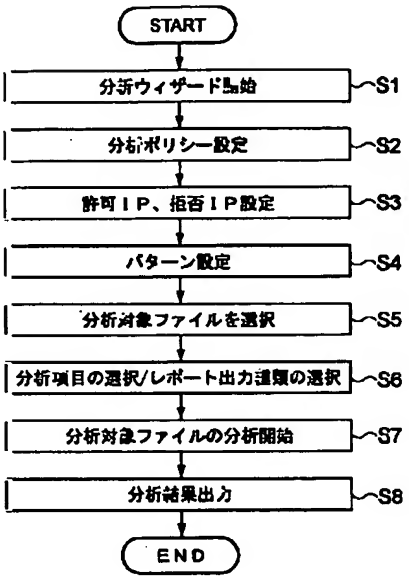
【図3】



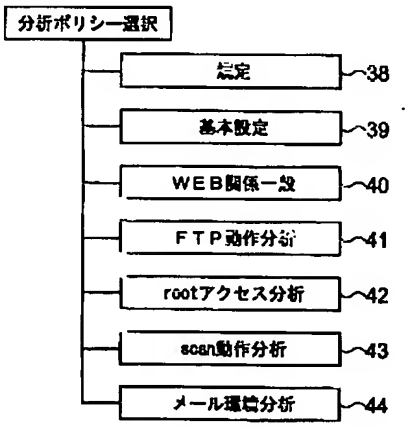
【図2】



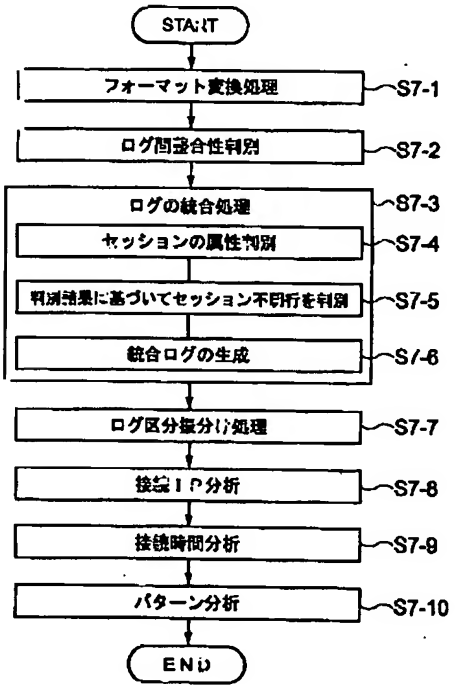
【図4】



【図5】



【図6】



【図8】

つ例3　動作確に引べた例1と例2

```
a-1    Feb 18 22:27:35 darkangel in.ftpd[2901]:connect from 210.232.105.***
a-2    Feb 18 22:27:40 darkangel ftpd[2901]:FTP LOGIN FROM:210.232.105.*** [210.232.105.***],root
b-1    Fri Feb 18 22:29:01 2000 1 210.232.105.*** 18732 /var/log/xxxxxx b_o r root ftp 0 *
b-2    Fri Feb 18 22:29:03 2000 1 210.232.105.*** 9635 /var/log/xxxx b_o r root ftp 0 *
b-3    Fri Feb 18 22:29:11 2000 1 210.232.105.*** 2517 /var/log/xxxxxx b_o r root ftp 0 *
b-4    Fri Feb 18 22:29:16 2000 1 210.232.105.*** 2830 /var/log/xxxxxx b_o r root ftp 0 *
a-3    Feb 18 22:27:42 darkangel ftpd[2901]:FTP session closed
```

【図7】

(a) ●例1 syslogによるftpの記録

a-1 Feb 18 22:27:35 darkangel in.ftpd[2901]:connect from 210.232.105.●●●
a-2 Feb 18 22:27:40 darkangel ftpd[2901]:FTP LOGIN FROM:210.232.105.●●● [210.232.105.●●●],root
a-3 Feb 18 22:27:42 darkangel ftpd[2901]:FTP session closed

●例2 例1当時のxferlogの記録

(b)
b-1 Fri Feb 18 22:29:01 2000 1 210.232.105.●●● 18732 /var/log/xxxxxx b_o r root ftp 0 *
b-2 Fri Feb 18 22:29:03 2000 1 210.232.105.●●● 8535 /var/log/xxxx b_o r root ftp 0 *
b-3 Fri Feb 18 22:29:11 2000 1 210.232.105.●●● 2517 /var/log/xxxxxxx b_o r root ftp 0 *
b-4 Fri Feb 18 22:29:16 2000 1 210.232.105.●●● 2930 /var/log/xxxxxx b_o r root ftp 0 *

【図9】

●例5 ・・・した例5

行ID	日付	・・・	サービス	PID	IP	アカウント	動作
a-1	Feb 18	22:27:35	in.ftpd	2901	210.232.105.●●●	-	connect from 210.232.105.●●●
a-2	Feb 18	22:27:40	ftpd	2901	210.232.105.●●●	root	FTP LOGIN FROM 210.232.105.●●● [210.232.105.●●●]
b-1	Feb 18	22:29:01	ftp	-	210.232.105.●●●	root	18732 /var/log/xxxxxx b_o r 0 *
b-2	Feb 18	22:29:03	ftp	-	210.232.105.●●●	root	8535 /var/log/xxxx b_o r 0 *
b-3	Feb 18	22:29:11	ftp	-	210.232.105.●●●	root	2517 /var/log/xxxxxxx b_o r 0 *
b-4	Feb 18	22:29:16	ftp	-	210.232.105.●●●	root	2930 /var/log/xxxxxx b_o r 0 *
a-3	Feb 18	22:27:42	ftpd	2901	-	-	FTP session closed

【図10】

●例4 /var/log/all.logの例

Oct 28 04:02:32 ●● sendmail[4427]: EAA04327: /var/●●●/●●●: ●●●●● directory path, marked ●●●●●
Oct 28 04:02:32 ●● sendmail[4427]: EAA04327: from=●●●, size=1619, class=0, pri=31619, nrcpts=1, ●●●●=<19991228192932.EAA04327@●, relay=●●●●●
Oct 28 04:02:32 ●● rmesg[4941]: rejected connection ●●●● server?
Oct 28 04:02:32 ●● sendmail[4944]: EAA04327: ●●●●●(●●●●): Cannot exec /bin/mail/●●●●●●●: ●●● a directory
Oct 28 04:02:32 ●● sendmail[4943]: EAA04327: to=●●●, ctladdr=●●●● (0/13), delay=00:00:00, ●●●●●=00:00:00, mailer=local, stat=Operating system error
Oct 28 04:02:32 ●● rmesg[4944]: rejected ●●●●●●●● ●●●● server?
Oct 28 04:02:33 ●● PAM_pwdb[4381]: (●●) session ●●●●● for user ●●●●● by (uid=0)
Oct 28 04:03:45 ●● PAM_pwdb[4381]: (●●) session ●●●●● for user ●●●●●
Oct 28 12:30:26 ●● in.●●●●●[4764]: connect from ●●●28-03.●●●●.●●●.●●.jp
Oct 28 12:30:36 ●● PAM_pwdb[4765]: (login) session opened for user bikmith by (uid=0)
Oct 28 12:30:36 ●● login[4765]: LOGIN ON ttyp0 BY bikmith FROM ●●●28-03.●●●●.●●●.●●.jp
(a) Oct 28 12:35:33 ●● PAM_pwdb[4765]: (login) session closed for user bikmith
Oct 28 12:35:43 ●● PAM_pwdb[4774]: (●●) session ●●●●● for user root by bikmith(uid=0)
Oct 28 12:50:33 ●● PAM_pwdb[4774]: (●●) session closed for user root
Oct 28 13:05:01 ●● ftpd[4892]: FTP LOGIN FROM ●●●28-03.●●●●.●●●.●●.jp [202.217.13.241], root
Oct 28 13:05:50 ●● in.ftpd[4892]: connect from ●●●28-03.●●●●.●●●.●●.jp
Oct 28 13:07:05 ●● in.●●●●●[4900]: connect from ●●●28-03.●●●●.●●●.●●.jp
Oct 28 13:07:15 ●● PAM_pwdb[4901]: (login) session opened for user bikmith by (uid=0)
Oct 28 13:07:18 ●● login[4901]: LOGIN ON ttyp0 BY bikmith from ●●●28-03.●●●●.●●●.●●.jp
Oct 28 13:07:15 ●● PAM_pwdb[4901]: (login) session closed for user bikmith
Oct 28 14:07:21 ●● PAM_pwdb[4912]: (●●) session opened for user root by bikmith(uid=0)
Oct 28 14:08:42 ●● PAM_pwdb[4913]: (●●) session closed for user root
Oct 28 14:08:01 ●● ftpd[4892]: FTP session closed

●例5 /var/log/auth.logの例

Oct 28 12:30:26 ●● in.●●●●●[4764]: connect from ●●●28-03.●●●●.●●●.●●.jp
(b) Oct 28 13:05:50 ●● in.ftpd[4892]: connect from ●●●28-03.●●●●.●●●.●●.jp
Oct 28 13:07:05 ●● in.●●●●●[4900]: connect from ●●●28-03.●●●●.●●●.●●.jp

【図16】

●例13

セッション名	PID	IP	接続時間
FTPセッション1	2901	210.190.79.139	Feb 18 22:27:35～Feb 18 22:31:02
FTPセッション2	2903	210.232.105.●●●	Feb 18 22:28:05～Feb 18 22:30:42
FTPセッション3	2907	210.232.105.●●●	Feb 18 22:30:50～Feb 18 22:69:22

【図11】

●例6 /var/log/info.logの内容

(a)

```
Feb 16 15:10:00 darkangel PAM_pwdb[3421]: 3 authentication failures: (uid=0) -> bikmith for login service
Feb 16 15:23:41 darkangel PAM_pwdb[3425]: (login) session opened for user bikmith by (uid=0)
Feb 16 15:23:41 darkangel login[3425]: LOGIN ON ttyp0 BY bikmith FROM p43-dn03.***.ne.jp
Feb 16 15:29:41 darkangel PAM_pwdb[3425]: (login) session closed for user bikmith
Feb 16 15:30:49 darkangel PAM_pwdb[3474]: (su) session opened for user root by bikmith(uid=0)
Feb 16 16:57:30 darkangel PAM_pwdb[3474]: (su) session closed for user root
```

●例7 /var/log/auth.logの内容

(b)

```
Feb 16 15:09:04 darkangel in.telnetd[3420]: connect from 210.154.165.244
Feb 16 15:09:21 darkangel login: FAILED LOGIN 1 FROM p51-dn09.***.ne.jp FOR bikmith, Authentication failure
Feb 16 15:09:42 darkangel login: FAILED LOGIN 2 FROM p51-dn09.***.ne.jp FOR bikmith, Authentication failure
Feb 16 15:10:00 darkangel login: TOO MANY LOGIN tRIES (3) FROM p51-dn09.***.ne.jp FOR bikmith, HAVE exhorted maximum number of retries for service.
Feb 16 15:10:11 darkangel in.telnetd[3422]: connect from 210.154.165.244
Feb 16 15:10:29 darkangel login: FAILED LOGIN 1 FROM p51-dn08.***.ne.jp FOR bikmith, Authentication failure
Feb 16 15:10:41 darkangel login: FAILED LOGIN 2 FROM p51-dn08.***.ne.jp FOR bikmith, Authentication failure
Feb 16 15:23:25 darkangel in.telnetd[3424]: connect from 210.154.184.108
Feb 16 15:23:32 darkangel login: FAILED LOGIN 1 FROM p43-dn03.***.ne.jp FOR bikmith, Authentication failure
```

【図12】

つ例8 /var/log/all.logの内容

```
Feb 16 15:09:04 darkangel in.telnetd[3420]: connect from 210.154.165.244
Feb 16 15:09:21 darkangel login: FAILED LOGIN 1 FROM p51-dn09.***.ne.jp FOR bikmith, Authentication failure
Feb 16 15:09:42 darkangel login: FAILED LOGIN 2 FROM p51-dn09.***.ne.jp FOR bikmith, Authentication failure
Feb 16 15:10:00 darkangel login: TOO MANY LOGIN TRIES (3) FROM p51-dn09.***.ne.jp FOR bikmith, HAVE exhorted maximum number of retries for service.
Feb 16 15:10:00 darkangel PAM_pwdb[3421]: 3 authentication failure: (uid=0) -> bikmith for login service
Feb 16 15:16:11 darkangel in.telnetd[3422]: connect from 210.154.165.244
Feb 16 15:16:29 darkangel login: FAILED LOGIN 1 FROM p18-dn08.***.ne.jp FOR bikmith, Authentication failure
Feb 16 15:16:41 darkangel login: FAILED LOGIN 2 FROM p18-dn08.***.ne.jp FOR bikmith, Authentication failure
Feb 16 15:23:25 darkangel in.telnetd[3424]: connect from 210.154.184.108
Feb 16 15:23:32 darkangel login: FAILED LOGIN 1 FROM p43-dn03.***.ne.jp FOR bikmith, Authentication failure
Feb 16 15:23:41 darkangel PAM_pwdb[3425]: (login) session opened for user bikmith by (uid=0)
Feb 16 15:23:41 darkangel login[3425]: LOGIN ON ttyp0 BY bikmith FROM p43-dn03.***.ne.jp
Feb 16 15:23:41 darkangel PAM_pwdb[3425]: (login) session closed for user bikmith
Feb 16 15:30:49 darkangel PAM_pwdb[3474]: (su) session opened for user root by bikmith (uid=0)
Feb 16 16:57:30 darkangel PAM_pwdb[3474]: (su) session closed for user root
```

【図13】

●例9 同時接続回線に複数のftpセッションがあるsyslogの例

(a)

```
a-1    Feb 18 22:27:35 darkangel in.ftpd[2901]: connect from 210.190.79.139
a-2    Feb 18 22:27:40 darkangel ftpd[2901]: FTP LOGIN FROM 210.190.79.139 [210.190.79.139], root
a-3    Feb 18 22:28:05 darkangel in.ftpd[2903]: connect from 210.232.105.***
a-4    Feb 18 22:28:09 darkangel ftpd[2903]: FTP LOGIN FROM 210.232.105.*** [210.232.105.***], root
a-5    Feb 18 22:30:42 darkangel ftpd[2903]: FTP session closed
a-6    Feb 18 22:30:50 darkangel in.ftpd[2907]: connect from 210.232.105.***
a-7    Feb 18 22:30:53 darkangel ftpd[2907]: FTP LOGIN FROM 210.232.105.*** [210.232.105.***], root
a-8    Feb 18 22:31:02 darkangel ftpd[2901]: FTP session closed
a-9    Feb 18 22:59:22 darkangel ftpd[2907]: FTP session closed
```

●例10 例10動作時のxferlog必記録

(b)

```
b-1    Fri Feb 18 22:29:01 2000 1 210.190.79.139 16732 /var/log/xxxxxx b _ o r root ftp 0 *
b-2    Fri Feb 18 22:29:03 2000 1 210.190.79.139 8435 /var/log/xxxx b _ o r root ftp 0 *
b-3    Fri Feb 18 22:30:55 2000 1 210.232.105.*** 2517 /var/log/xxxxxxx b _ o r root ftp 0 *
b-4    Fri Feb 18 22:30:57 2000 1 210.232.105.*** 2920 /var/log/xxxxxx b _ o r root ftp 0 *
b-5    Fri Feb 18 22:31:01 2000 1 210.190.79.139 18 /var/log/xxxxxx b _ o r root ftp 0 *
b-6    Fri Feb 18 22:35:03 2000 1 210.232.105.*** 8835 /var/log/xxxx b _ o r root ftp 0 *
```

【図14】

つ例11

行ID	日付	時刻	サービス	PID	IP	アカウント	動作
a-1	Feb 18	22:27:35	in.ftpd	2901	210.190.79.139	-	connect from 210.190.79.139
a-2	Feb 18	22:27:40	ftpd	2901	210.190.79.139	root	FTP LOGIN FROM 210.190.79.139 [210.190.79.139]
a-3	Feb 18	22:28:05	in.ftpd	2903	210.232.105.***	-	connect from 210.232.105.***
a-4	Feb 18	22:28:09	ftpd	2903	210.232.105.***	root	FTP LOGIN FROM 210.232.105.***[210.232.105.***]
b-1	Feb 18	22:29:01	ftp	-	210.190.79.139	root	18732 /var/log/xxxxxx b_o r 0 *
b-2	Feb 18	22:29:03	ftp	-	210.190.79.139	root	8636 /var/log/xxxx b_o r 0 *
a-5	Feb 18	22:30:42	ftpd	2903	-	-	FTP session closed
a-6	Feb 18	22:30:50	in.ftpd	2907	210.232.105.***	-	connect from 210.232.105.***
a-7	Feb 18	22:30:53	ftpd	2907	210.232.105.***	root	FTP LOGIN FROM 210.232.105.***[210.232.105.***]
b-3	Feb 18	22:30:55	ftp	-	210.232.105.***	root	2517 /var/log/xxxxxx b_o r 0 *
b-4	Feb 18	22:30:57	ftp	-	210.232.105.***	root	2930 /var/log/xxxxxx b_o r 0 *
b-5	Feb 18	22:31:01	ftp	-	210.190.79.139	root	18 /var/log/xxxxxx b_o r 0 *
a-8	Feb 18	22:31:02	ftpd	2901	-	-	FTP session closed
b-6	Feb 18	22:35:03	ftp	-	210.232.105.***	root	8535 /var/log/xxxx b_o r 0 *
a-9	Feb 18	22:59:22	ftpd	2907	-	-	FTP session closed

【図15】

●例12

(a)

・FTPセッション1(PID=2901)

行ID	日付	時刻	サービス	PID	IP	アカウント	動作
a-1	Feb 18	22:27:35	in.ftpd	2901	210.190.79.139	-	connect from 210.190.79.139
a-2	Feb 18	22:27:40	ftpd	2901	210.190.79.139	root	FTP LOGIN FROM 210.190.79.139 [210.190.79.139]
a-8	Feb 18	22:31:02	ftpd	2901	-	-	FTP session closed

(b)

・FTPセッション2(PID=2903)

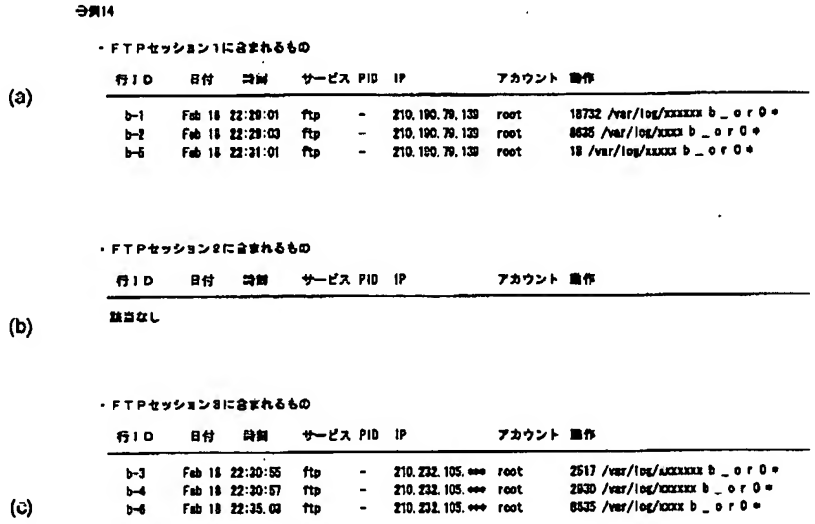
行ID	日付	時刻	サービス	PID	IP	アカウント	動作
a-3	Feb 18	22:28:05	in.ftpd	2903	210.232.105.***	-	connect from 210.232.105.***
a-4	Feb 18	22:28:09	ftpd	2903	210.232.105.***	root	FTP LOGIN FROM 210.232.105.***[210.232.105.***]
a-5	Feb 18	22:30:42	ftpd	2903	-	-	FTP session closed

(c)

・FTPセッション3(PID=2907)

行ID	日付	時刻	サービス	PID	IP	アカウント	動作
a-6	Feb 18	22:30:50	in.ftpd	2907	210.232.105.***	-	connect from 210.232.105.***
a-7	Feb 18	22:30:53	ftpd	2907	210.232.105.***	root	FTP LOGIN FROM 210.232.105.***[210.232.105.***]
a-9	Feb 18	22:59:22	ftpd	2907	-	-	FTP session closed

【図17】



例14

・FTPセッション1に含まれるもの

(a)

行ID	日付	時刻	サービス	PID	IP	アカウント	動作
b-1	Feb 18	22:29:01	ftp	-	210.190.79.139	root	18732 /var/log/xxxxxx b _ o r 0 *
b-2	Feb 18	22:29:03	ftp	-	210.190.79.139	root	8635 /var/log/xxxx b _ o r 0 *
b-5	Feb 18	22:31:01	ftp	-	210.190.79.139	root	18 /var/log/xxxxx b _ o r 0 *

・FTPセッション2に含まれるもの

(b)

行ID	日付	時刻	サービス	PID	IP	アカウント	動作

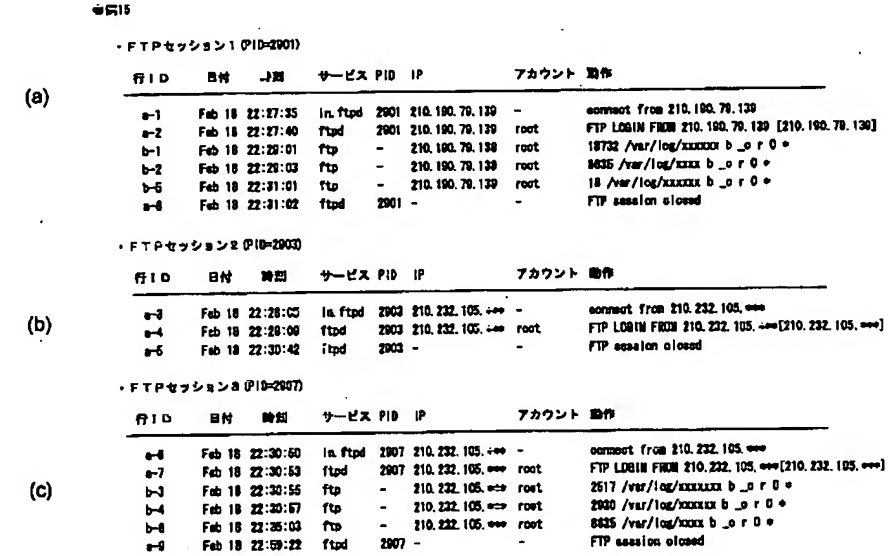
該当なし

・FTPセッション3に含まれるもの

(c)

行ID	日付	時刻	サービス	PID	IP	アカウント	動作
b-3	Feb 18	22:30:55	ftp	-	210.232.105.***	root	2517 /var/log/xxxxxx b _ o r 0 *
b-4	Feb 18	22:30:57	ftp	-	210.232.105.***	root	2930 /var/log/xxxxxx b _ o r 0 *
b-6	Feb 18	22:35:03	ftp	-	210.232.105.***	root	8635 /var/log/xxxx b _ o r 0 *

【図18】



例15

・FTPセッション1 (PID=2901)

(a)

行ID	日付	時刻	サービス	PID	IP	アカウント	動作
a-1	Feb 18	22:27:35	in.ftpd	2901	210.190.79.139	-	connect from 210.190.79.139
a-2	Feb 18	22:27:40	ftpd	2901	210.190.79.139	root	FTP LOGIN FROM 210.190.79.139 [210.190.79.139]
b-1	Feb 18	22:29:01	ftp	-	210.190.79.139	root	18732 /var/log/xxxxxx b _o r 0 *
b-2	Feb 18	22:29:03	ftp	-	210.190.79.139	root	8635 /var/log/xxxx b _o r 0 *
b-5	Feb 18	22:31:01	ftp	-	210.190.79.139	root	18 /var/log/xxxxxx b _o r 0 *
a-8	Feb 18	22:31:02	ftpd	2901	-	-	FTP session closed

・FTPセッション2 (PID=2903)

(b)

行ID	日付	時刻	サービス	PID	IP	アカウント	動作
a-3	Feb 18	22:28:05	in.ftpd	2903	210.232.105.***	-	connect from 210.232.105.***
a-4	Feb 18	22:28:09	ftpd	2903	210.232.105.***	root	FTP LOGIN FROM 210.232.105.***[210.232.105.***]
a-5	Feb 18	22:30:42	ftpd	2903	-	-	FTP session closed

・FTPセッション3 (PID=2907)

(c)

行ID	日付	時刻	サービス	PID	IP	アカウント	動作
a-6	Feb 18	22:30:50	in.ftpd	2907	210.232.105.***	-	connect from 210.232.105.***
a-7	Feb 18	22:30:53	ftpd	2907	210.232.105.***	root	FTP LOGIN FROM 210.232.105.***[210.232.105.***]
b-3	Feb 18	22:30:55	ftp	-	210.232.105.***	root	2517 /var/log/xxxxxx b _o r 0 *
b-4	Feb 18	22:30:57	ftp	-	210.232.105.***	root	2930 /var/log/xxxxxx b _o r 0 *
b-6	Feb 18	22:35:03	ftp	-	210.232.105.***	root	8635 /var/log/xxxx b _o r 0 *
a-9	Feb 18	22:59:22	ftpd	2907	-	-	FTP session closed